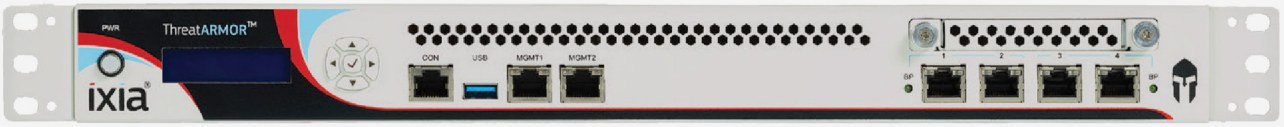
ThreatARMOR™

ixia
A Keysight Business

УСТРОЙСТВО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, УСИЛИВАЮЩЕЕ ЗАЩИТУ СЕТИ ОТ КИБЕРАТАК



Простое в использовании устройство ThreatARMOR компании Ixia предназначено для блокирования нежелательного входящего трафика с огромного числа известных IP-адресов проблемных сайтов или даже целых стран и предотвращения исходящих от компьютеров защищаемой сети соединений с вредоносными сайтами. ThreatARMOR существенно снижает нагрузку на другие защитные устройства (например, на межсетевой экран и систему IPS) и специалистов по информационной безопасности (ИБ), что способствует повышению эффективности их работы.

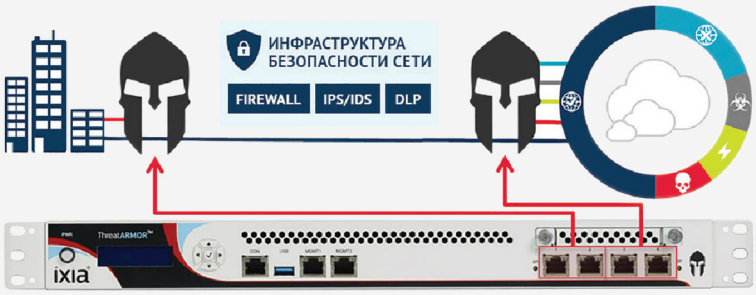
Основные функции и достоинства ThreatARMOR

- Уменьшение поверхности атаки сети (совокупности всевозможных путей проникновения в сеть).
- Блокировка нежелательного входящего трафика из Интернета и предотвращение исходящих от компьютеров защищаемой сети соединений с фишинговыми сайтами и контроллерами ботнетов.
- Отсутствие ложно-позитивных сообщений.
- Постоянное получение обновлений от облачного сервиса Application and Threat Intelligence (ATI) Research Center.
- Наличие двух блоков питания с взаимным резервированием и режима bypass (для сохранения работоспособности контролируемых линий связи).

Снижение нагрузки на устройства ИБ и сокращение поверхности атаки сети

Устройство ThreatARMOR можно задействовать для контроля IP-трафика до и после имеющейся инфраструктуры безопасности сети. При этом оно будет отсекать заведомо вредоносный и не нужный для ведения бизнеса входящий трафик из Интернета (по заранее известным IP-адресам) и предотвращать исходящие от компьютеров защищаемой сети соединения с фишинговыми сайтами и контроллерами ботнетов. ThreatARMOR быстро определяет инфицированные компьютеры в защищаемой сети.

IXIA THREATARMOR – УСТРОЙСТВО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, УСИЛИВАЮЩЕЕ ЗАЩИТУ СЕТИ ОТ КИБЕРАТАК



Отфильтровывая заведомо нежелательный входящий трафик, который не нужно анализировать, устройство ThreatARMOR снижает нагрузку на анализирующие трафик устройства ИБ (межсетевой экран, различные сетевые анализаторы и др.) и сокращает поверхность атаки сети. Контроль трафика (с блокированием многочисленных IP-адресов) данное устройство осуществляет на полной линейной скорости своих портов (1 или 10 Гбит/с).

Уменьшение усталости от оповещений

Хакерские атаки становятся все более сложными и изощренными, растет число этих атак, поэтому многие предприятия для борьбы с угрозами ИБ используют все более мощные и многофункциональные устройства анализа трафика и предотвращения вторжений. По оценкам института Понемона (Ponemon Institute) предприятия тратят в среднем 21 тыс. часов в год на обработку ложно-позитивных сообщений о киберугрозах, поступающих от этих устройств. Не пропуская заведомо нежелательный трафик на устройства анализа трафика, продукт ThreatARMOR примерно на 30% снижает число ложно-позитивных сообщений и таким образом обеспечивает значительную экономию временных и денежные затрат заказчиков на рассмотрение потока излишних оповещений. При этом само устройство ThreatARMOR работает на основе получаемой в рамках программы ATI точной информации об угрозах ИБ и поэтому не выдает ложно-позитивных сообщений.

Чрезмерное число оповещений вызывает усталость от них, в результате чего специалисты по ИБ могут пропускать критически важные оповещения. ThreatARMOR повышает эффективность использования средств обеспечения ИБ и минимизирует риск пропуска критически важных оповещений.

Поддержка в рамках программы ATI

Команда специалистов компании Ixia, реализующая программу технической поддержки Application and Threat Intelligence (ATI), имеет более чем десятилетний опыт анализа работы различных сетевых приложений и тестирования защиты сетей крупнейших сервис-провайдеров и компаний-производителей. Используя передовые методы контроля сетей для захвата и идентификации трафика новых легитимных и вредоносных приложений, эти специалисты накапливают информацию о приложениях и угрозах ИБ и снабжают ею заказчиков.

В рамках программы ATI компания Ixia предоставляет своим заказчикам все необходимое для тщательного тестирования производительности, безопасности и стабильности их ИТ-инфраструктур. К этому относится предоставление доступа к ПО для имитации работы приложений, хакерских атак и расширения функционала решений Ixia. Также оказывается полный спектр услуг технической поддержки и технического обслуживания. Благодаря этой программе, происходит постоянное обновление функционала используемого заказчиками оборудования и ПО компании Ixia.

Получая информацию о приложениях и/или угрозах ИБ в рамках программы ATI, устройства ThreatARMOR могут сокращать поверхность атаки защищаемой сети, модули ATI Processor – контролировать работу приложений, а тестовые комплексы на базе ПО BreakingPoint, IxLoad или IxNetwork – испытывать сетевые решения реалистичным трафиком приложений и атак.

В соответствии с программой ATI, устройства ThreatARMOR снабжаются не только информацией об угрозах ИБ, но и детальными отчетами Rap Sheet (в переводе – досье преступника), в которых задокументирована опасная активность (например, распространение вредоносного ПО или фишинг) по каждому блокируемому сайту. Перечень вредоносных сайтов в устройстве ThreatARMOR постоянно актуализируется облачным сервисом исследовательского центра ATI Research Center, который передает обновления каждые 5 минут.

Надежность и простота

Устройство ThreatARMOR предназначено для включения в разрывы линий связи (in-band). (Возможна и пассивная инсталляция данного устройства с подключением к сети через ответвители или SPAN-порты.) Чтобы не снижать надежность работы линий связи, сетевые порты устройства поддерживают обходной режим (bypass). Благодаря этому, в случае прекращения подачи электропитания на ThreatARMOR передача трафика по контролируемым линиям не будет прекращена. Для повышения отказоустойчивости устройство оснащено двумя блоками питания с возможностью горячей замены и заменяемым на месте эксплуатации твердотельным диском (SSD).

Устанавливать устройство ThreatARMOR очень просто: нужно лишь подключить его к линиям связи и электрическим розеткам и выбрать режим Report Only Mode или Blocking Mode. Далее оно автоматически начнет получать информацию об угрозах ИБ и блокировать трафик вредоносных сайтов. В устройстве имеется опциональная функция географической блокировки. Она не позволяет трафику из указанных заказчиком стран входить в его сеть. При этом сохраняется возможность обращаться к информационным сайтам в этих странах из защищаемой сети.

Управляют устройством ThreatARMOR посредством консольного последовательного порта, ЖК-дисплея и клавиш, расположенных на передней панели. Там же находятся два управляющих Ethernet-интерфейса.

ThreatARMOR – устанавливаемое в 19-дюймовую стойку небольшое (высотой 1U) устройство массой 10 кг. Оно предназначено для эксплуатации в диапазоне температур окружающей среды от +5 до +40 °C при относительной влажности от 10 до 85% (без конденсации). Диапазон температур хранения устройства: от -20 до +75 °C.

IXIA WORLDWIDE
26601 W. AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942
(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 818.871.1805
www.ixiacom.com

IXIA EUROPE
CLARION HOUSE, NORREYS
DRIVE MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127